Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 124 (2007) 364–379

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

On the equation $y^2 = x(x - 2^m)(x + q - 2^m)$ ☆

Andrzej Dąbrowski *, Małgorzata Wieczorek

Institute of Mathematics, University of Szczecin, ul. Wielkopolska 15, 70-451 Szczecin, Poland

Received 10 July 2003; revised 9 November 2005

Available online 13 November 2006

Communicated by David Goss

Abstract

Consider a family of elliptic curves $E_{q,m}$: $y^2 = x(x - 2^m)(x + q - 2^m)$, where q is an odd prime satisfying $q - 2^m > 0$. In a case $q - 2^m$ is a prime, we give fairly complete formula for the rank, and describe an elementary method to search for non-trivial points. In general case we can prove that either the rank or 2-part of the Tate–Shafarevich group can be arbitrarily large. We also prove (under reasonable assumptions) that for any partition $k = l + n$ into non-negative integers there are pairwise nonisogeneous elliptic curves $E_1, \ldots, E_k$ among $E_{q,m}$'s such that for a positive proportion of prime quadratic twists by p we have: $\operatorname{rank} E_1^{(p)} = \cdots = \operatorname{rank} E_l^{(p)} = 0$ and $\operatorname{rank} E_{l+1}^{(p)} = \cdots = \operatorname{rank} E_k^{(p)} = 1$. We prove explicit estimates for the canonical height on (quadratic twists of) $E_{q,m}$ (in a case $q - 2^m$ is a prime) and include a list of values of the analytic order of Ш.

MSC: 14G10; 14G05

1. Introduction

It is believed that there exist infinitely many twin primes. More generally, one expect that, for fixed even integer $k \geqslant 2$, there exist infinitely many primes p such that $p + k$ is a prime (first part of Conjecture B in [6]). We shall need the following (rather weak) form of the conjecture.

☆ Research partially supported by KBN Grant No. 2P03A04922.

* Corresponding author.

E-mail addresses: dabrowsk@sus.univ.szczecin.pl (A. Dąbrowski), wieczorek@sus.univ.szczecin.pl (M. Wieczorek).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.09.005

Conjecture B_0. *For any pair $(m, i) \in \mathbb{N} \times \{1, 3, 5, 7\}$ there exists a prime $q \equiv i \pmod 8$ such that $q - 2^m$ is a prime.*

Let q, p be odd primes satisfying $q - 2^m = p$. We are concerned with determining the rank of the associated elliptic curve $E_{q,p,m}$: $y^2 = x(x - 2^m)(x + p)$. Proposition 4.19 in [9] implies the upper bound $\operatorname{rank} E_{q,p,m}(\mathbb{Q}) \leqslant 2$. Moreover, this bound can only be attained for $m = 3$ or $m \geqslant 5$ and certain special primes $q \equiv 1 \pmod 8$.

We can determine the $\mathbb{Q}$-rank $r_{q,p,m}$ of $E_{q,p,m}$ as follows. Let $E'_{q,p,m}$: $y^2 = x^3 + 2(2^m - p)x^2 + q^2x$ be the isogeneous curve, where the two-isogeny $\phi : E_{q,p,m} \to E'_{q,p,m}$ is defined by $\phi((x, y)) = (y^2/x^2, -y(2^m p + x^2)/x^2)$; let $\hat{\phi}$ denote the dual isogeny. Let $Ш(E_{q,p,m}/\mathbb{Q})$ (respectively $Ш(E'_{q,p,m}/\mathbb{Q})$) denote the Shafarevich–Tate group of $E_{q,p,m}$ (respectively of $E'_{q,p,m}$).

Theorem 1. *We have*

(i) $r_{q,p,m} = 0$, *if* $p \equiv 3, 5 \pmod 8$, $m = 1$ *or* $p \equiv 3 \pmod 4$, $m = 2, 3$;
(ii) $r_{q,p,m} + \dim_2 Ш(E'_{q,p,m}/\mathbb{Q})[2] = 1$, *if* $p \equiv 1 \pmod 8$, $m = 1, 2$ *or* $p \equiv 5 \pmod 8$, $m = 3$ *or* $m = 4$ *or* $p \equiv 3, 5 \pmod 8$, $m \geqslant 5$ *or* $p \equiv 7 \pmod 8$, *even* $m \geqslant 6$;
(iii) $r_{q,p,m} + \dim_2 Ш(E'_{q,p,m}/\mathbb{Q})[2] = 2$, *if* $p \equiv 5 \pmod 8$, $m = 2$ *or* $p \equiv 1 \pmod 8$, *even* $m \geqslant 6$;
(iv) $r_{q,p,m} + \dim_2 Ш(E_{q,p,m}/\mathbb{Q})[2] = 1$, *if* $p \equiv 7 \pmod 8$, odd $m \neq 3$;
(v) *For odd* $m \geqslant 3$ *and* $p \equiv 1 \pmod 8$ *we have*

$$r_{q,p,m} + \dim_2 Ш(E_{q,p,m}/\mathbb{Q})[\phi] + \dim_2 Ш\big(E'_{q,p,m}/\mathbb{Q}\big)[\hat{\phi}] = 2.$$

The result is the same statement as Proposition 6.2 in [16], but for a slightly more complicated family of elliptic curves, and the proof follows the same line.

Corollary 1. *We have the following formulas for the rank*:

(i) $r_{q,p,1} \leqslant 1$; $r_{q,p,1} = 0$ *if* $p \equiv 3, 5 \pmod 8$.
(ii) $r_{q,p,2} \leqslant 1$; $r_{q,p,2} = 0$ *if* $p \equiv 3, 7 \pmod 8$.
(iii) $r_{q,p,3} = 0$ *if* $p \equiv 3 \pmod 4$.
(iv) $r_{q,p,4} \leqslant 1$.

Let $\epsilon(E)$ be the global root number of an elliptic curve E over rationals. It is equal to the sign of the functional equation of the L-function $L(E, s)$. The parity conjecture states that

$$\epsilon(E) = (-1)^{r_E},$$

where r_E denotes the rank of $\mathbb{Q}$-points of E.

Corollary 2. *Assume the parity conjecture holds true for the family $E_{q,p,m}$. Then*

(i) $r_{q,p,1} = 1$ *if* $p \equiv 1, 7 \pmod 8$.
(ii) $r_{q,p,2} = 1$ *if* $p \equiv 1 \pmod 8$.
(iii) $r_{q,p,2} = 0$ *if* $p \equiv 5 \pmod 8$.
(iv) $r_{q,p,3} = 1$ *if* $p \equiv 5 \pmod 8$.

(v) $r_{q,p,4} = 1$.
(vi) $r_{q,p,m} = 1$ $(m \geqslant 5)$ *if* $p \equiv 3, 5, 7 \pmod 8$.

In the remaining case $p \equiv 1 \pmod 8$ and $m = 3$ or $m \geqslant 5$, the parity conjecture implies $r_{q,p,m} = 0$ or 2. Actually, both cases do appear: $r_{97,89,3} = r_{353,97,8} = 0$ and $r_{409,401,3} = r_{449,193,8} = 2$.

Proof of Theorem 1, based on the 2-descent method, is given in Sections 2 and 4. Proof of Corollary 2 reduces to calculations of the global root numbers (see Section 3). Numerical calculations, based on Theorem 1 (and corollaries), suggest that about 69% of the curves $E_{q,p,m}$ have rank 1 (see Section 6). We describe an elementary method to search for non-torsion points in $E_{q,p,m}(\mathbb{Q})$ in Section 5.

Fix a positive integer m. For any odd prime q satisfying $q - 2^m > 0$ consider an elliptic curve $E_{q,m}\colon\ y^2 = x(x - 2^m)(x + q - 2^m)$. Let $r_{q,m} := \operatorname{rank} E_{q,m}(\mathbb{Q})$. Section 6 contains numerical investigations related to the rank $r_{q,m}$ in a case $q - 2^m = p_1 p_2$ (p_1, p_2 different rational primes). In a general case we can prove the following result.

Theorem 2. *Assume* $q - 2^m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, *with primes* $q, p_1, \ldots, p_n$ *satisfying* $p_i \equiv 1 \pmod 8$ $(i = 1, \ldots, k,\ k \leqslant n)$, *and even* m. *If* $(\frac{p_i}{p_j}) = 1$ *for* $i, j = 1, \ldots, k$ $(i \neq j)$, *then*

$$r_{q,m} + \dim_2 Ш\left(E'_{q,m}/\mathbb{Q}\right)[2] \geqslant k - 1.$$

Using the Dirichlet theorem on primes in arithmetic progressions we conclude that, either $r_{q,m}$ or $\dim_2 Ш(E'_{q,m}/\mathbb{Q})[2]$ can be arbitrarily large.

It is widely believed that a positive proportion of quadratic twists $E^{(d)}$ (d square-free) of a fixed elliptic curve E over $\mathbb{Q}$ has rank zero (proved by Iwaniec and Sarnak [8] under the Riemann hypothesis), but this is only known for special cases. The best unconditional result is due to Ono and Skinner [13]; they also proved that for an elliptic curve E with conductor $\leqslant 100$, a positive proportion of the prime quadratic twists $E^{(-p)}$ has rank zero.

Let $M^k_{E_{q,p,m}}(X) := \sharp\{\text{primes}\, r \leqslant X\colon \operatorname{rank} E^{(r)}_{q,p,m}(\mathbb{Q}) = k\}$. We will prove the following qualitative results.

Theorem 3. *Fix odd primes* q, p *satisfying* $q - 2^m = p$.

(i) *Assume* $q \not\equiv 1 \pmod 8$ *or* $q \equiv 1 \pmod 8$ *and* $m \in \{1, 2, 3\}$. *Then we have*

$$M^0_{E_{q,p,m}}(X) \gg \frac{X}{\log X}.$$

(ii) *Assume the parity conjecture holds true for prime quadratic twists* $E^{(r)}_{q,p,m}$. *Then*

$$M^1_{E_{q,p,m}}(X) \gg \frac{X}{\log X}.$$

Method of proof of Theorem 3 leads to the following result (compare [2], where similar results and conjectures are discussed in a case $k = 2$). Let $\mathbb{E}_m$ be the set consisting of all the curves $E_{q,p,m}$; put $\mathbb{E} := \bigcup_{m \geqslant 1} \mathbb{E}_m$.

Theorem 4. *Fix an integer $k \geqslant 2$.*

(i) *Assume there exist infinitely many twin primes. There are pairwise nonisogeneous elliptic curves $E_1, \dots, E_k \in \mathbb{E}_1$ such that a positive proportion of prime quadratic twists $E_1^{(p)}, \dots, E_k^{(p)}$ has rank zero.*

(ii) *Assume there exist infinitely many twin primes, and the parity conjecture holds true for prime quadratic twists of curves from $\mathbb{E}_1$. There are pairwise nonisogeneous elliptic curves $E_1, \dots, E_k \in \mathbb{E}_1$ such that a positive proportion of quadratic twists $E_1^{(p)}, \dots, E_k^{(p)}$ has rank one.*

(iii) *Assume Conjecture B_0 and the parity conjecture for prime quadratic twists of curves from $\mathbb{E}$ hold true. For any partition $k = l+n$ into the sum of integers $l > 0$, $n > 0$, there are pairwise nonisogeneous curves $E_1, \dots, E_k \in \mathbb{E}$ such that for a positive proportion of primes p we have* $\operatorname{rk} E_1^{(p)} = \cdots = \operatorname{rk} E_l^{(p)} = 0$ *and* $\operatorname{rk} E_{l+1}^{(p)} = \cdots = \operatorname{rk} E_k^{(p)} = 1$.

2. Computation of the Selmer groups

2.1. The case of odd primes p, q satisfying $q - 2^m = p$

Let

$$E'_{q,p,m}\colon\ y^2 = x^3 + 2\big(2^m - p\big)x^2 + q^2 x.$$

Consider the two-isogeny $\phi : E_{q,p,m} \to E'_{q,p,m}$ defined by

$$\phi((x,y)) = \big(y^2/x^2, -y\big(2^m p + x^2\big)/x^2\big);$$

let $\hat{\phi}$ denote the dual isogeny. In this section, we compute the Selmer groups $S^{(\phi)}(E_{q,p,m}/\mathbb{Q})$ and $S^{(\hat{\phi})}(E'_{q,p,m}/\mathbb{Q})$.

Put $S = \{\infty, 2, p, q\}$, and $\mathbb{Q}(S,2) = \{\pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq\}$. Let

$$C_d(q,p,m)\colon\ dy^2 = d^2 - 2d\big(p - 2^m\big)x^2 + q^2x^4,$$
$$C'_d(q,p,m)\colon\ dy^2 = d^2 + 4d\big(p - 2^m\big)x^2 - 2^{m+4}px^4.$$

Using Proposition 4.9 in [16], we have the following identifications:

$$S^{(\phi)}(E_{q,p,m}/\mathbb{Q}) \simeq \big\{d \in \mathbb{Q}(S,2)\colon\ C_d(q,p,m)(\mathbb{Q}_l) \neq \emptyset \text{ for all } l \in S\big\},$$
$$S^{(\hat{\phi})}\big(E'_{q,p,m}/\mathbb{Q}\big) \simeq \big\{d \in \mathbb{Q}(S,2)\colon\ C'_d(q,p,m)(\mathbb{Q}_l) \neq \emptyset \text{ for all } l \in S\big\}.$$

Proposition 1. *We have*

(i) $S^{(\phi)}(E_{q,p,m}/\mathbb{Q}) \simeq \{0\}$ *for odd $m \geqslant 5$ and $p \equiv 3, 5 \pmod 8$ or $m = 1$ and $p \equiv 1, 3, 5 \pmod 8$ or $m = 3$ and $p \equiv 3, 5, 7 \pmod 8$; $S^{(\phi)}(E_{q,p,m}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ in other cases.*

(ii) $S^{(\hat{\phi})}(E'_{q,p,m}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ *for $m = 2$ and $p \equiv 3, 7 \pmod 8$; $S^{(\hat{\phi})}(E'_{q,p,m}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^3$ for $m \geqslant 1$, $m \neq 2, 4$ and $p \equiv 1 \pmod 8$ or $m = 2, 3$ and $p \equiv 5 \pmod 8$ or odd $m \geqslant 5$ and $p \equiv 3, 5 \pmod 8$; $S^{(\hat{\phi})}(E'_{q,p,m}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ in other cases.*

Proof. (i) Of course $C_d(q,p,m)(\mathbb{R}) = \emptyset$ for $d < 0$, and $C_d(q,p,m)(\mathbb{R}) \neq \emptyset$ for $d > 0$. Suppose next that $d = 2k$ with $k = 1, p, q, pq$ and that $C_{2k}(q,p,m)(\mathbb{Q}_2) \neq \emptyset$. Taking the valuation v_2 at 2 of both sides, we obtain $v_2(\text{LHS})$ is odd (or ∞), while $v_2(\text{RHS})$ is even, a contradiction. Similarly, $C_p(q,p,m)(\mathbb{Q}_p) = \emptyset$ and $C_{pq}(q,p,m)(\mathbb{Q}_p) = \emptyset$. Of course, $C_1(q,p,m)(\mathbb{Q}_l) \neq \emptyset$ ($l \in S$). We now investigate the last case:

$$C_q(q,p,m)\colon\ y^2 = q - 2\big(q - 2^{m+1}\big)x^2 + qx^4.$$

First note, that $C_q(q,p,m)(\mathbb{Q}_l) \neq \emptyset$ implies $C_q(q,p,m)(\mathbb{Z}_l) \neq \emptyset$. Indeed, $(x,y) \in C_q(q,p,m)(\mathbb{Q}_l)$ implies $(1/x, y/x^2) \in C_q(q,p,m)(\mathbb{Q}_l)$. Moreover, if m is even, then $C_q(q,p,m)(\mathbb{Q}_l) \neq \emptyset$ for any $l \in S$. If m is odd, then $C_q(q,p,m)(\mathbb{Q}_q) \neq \emptyset$ if and only if $q \equiv 1, 7 \pmod 8$, and $C_q(q,p,m)(\mathbb{Q}_p) \neq \emptyset$ if and only if $p \equiv 1, 7 \pmod 8$. If $q \equiv 1 \pmod 8$, then using Hensel's Lemma we immediately obtain $C_q(q,p,m)(\mathbb{Q}_2) \neq \emptyset$. If $q \equiv 7 \pmod 8$ and $m = 2k+1$, $k \geqslant 2$, then $(1 + 2^k t_0, 2^{k+1} u_0) \in C_q(q,p,m)(\mathbb{Q}_2)$, with $t_0, u_0 \in \mathbb{Z}_2^\times$. In the remaining cases we have $C_q(q,p,m)(\mathbb{Q}_2) = \emptyset$. This proves part (i).

(ii) Of course, $C'_d(q,p,m)(\mathbb{R}) \neq \emptyset$ for $d \in \mathbb{Q}(S,2)$. Let $d \in \{\pm q, \pm 2q, \pm pq, \pm 2pq\}$, and suppose $C'_d(q,p,m)(\mathbb{Q}_q) \neq \emptyset$. Taking the valuation v_q at q of both sides, we obtain $v_q(\text{LHS})$ is odd (or ∞), while $v_q(\text{RHS})$ is even, a contradiction.

Of course, $C'_1(q,p,m)(\mathbb{Q}_l) \neq \emptyset$ and $C'_{-p}(q,p,m)(\mathbb{Q}_l) \neq \emptyset$ for $l \in S$. It is plain, that $C'_d(q,p,m)(\mathbb{Q}_p) \neq \emptyset$ for $d \in \{-1, \pm 2, p, \pm 2p\}$. Over $\mathbb{Q}_q$ we have (we abbreviate $C'_d = C'_d(q,p,m)$):

$$\begin{aligned}
C'_{-1}(\mathbb{Q}_q) \neq \emptyset &\iff \left(\frac{-1}{q}\right) = 1 \text{ or } \left(\frac{-2^m}{q}\right) = 1,\\
C'_{2}(\mathbb{Q}_q) \neq \emptyset &\iff \left(\frac{2^{m+1}}{q}\right) = 1,\\
C'_{-2}(\mathbb{Q}_q) \neq \emptyset &\iff \left(\frac{-2}{q}\right) = 1 \text{ or } \left(\frac{-2^{m+1}}{q}\right) = 1,\\
C'_{p}(\mathbb{Q}_q) \neq \emptyset &\iff \left(\frac{-1}{q}\right) = 1 \text{ or } \left(\frac{-2^m}{q}\right) = 1,\\
C'_{2p}(\mathbb{Q}_q) \neq \emptyset &\iff \left(\frac{-2}{q}\right) \text{ or } \left(\frac{-2^{m+1}}{q}\right) = 1,\\
C'_{-2p}(\mathbb{Q}_q) \neq \emptyset &\iff \left(\frac{2^{m+1}}{q}\right) = 1.
\end{aligned}$$

Let us summarize the calculations:

$$S^{(\hat{\phi})}\big(E'_{q,p,m}/\mathbb{Q}\big) \subset \begin{cases} \{1, 2, -p, -2p\} & \text{for } q \equiv 7 \pmod 8,\\ \{1, -2, -p, 2p\} & \text{for even } m \text{ and } q \equiv 3 \pmod 8,\\ \{\pm 1, \pm p\} & \text{for even } m \text{ and } q \equiv 5 \pmod 8,\\ \{\pm 1, \pm 2, \pm p, \pm 2p\} & \text{in other cases.} \end{cases}$$

To finish the proof of part (ii) it remains to investigate the situation over $\mathbb{Q}_2$.

Considering 2-adic valuations, we obtain $-1 \notin S^{(\hat{\phi})}(E'_{q,p,m}/\mathbb{Q})$ if $m = 1$ and $q \equiv 1, 5 \pmod 8$ or $m = 3$ and $q \equiv 3 \pmod 8$. On the other hand, taking $y = 0$, we obtain $C'_{-1}(\mathbb{Q}_2) \neq \emptyset$ if $p \equiv 1 \pmod 8$. The remaining cases follow the same line. We omit the details.

Let us summarize the final calculations:

$$S^{(\hat{\phi})}\big(E'_{q,p,m}/\mathbb{Q}\big) = \begin{cases} \{1, -p\} & \text{for } m = 2 \text{ and } q \equiv 3, 7 \pmod 8, \\ \{1, -2, -p, 2p\} & \text{for even } m \geqslant 4 \text{ and } q \equiv 3 \pmod 8, \\ \{\pm 1, \pm p\} & \text{for even } m \text{ and } q \equiv 5 \pmod 8 \text{ or} \\ & m = 4 \text{ and } q \equiv 1 \pmod 8, \\ \{1, 2, -p, -2p\} & \text{for } m \geqslant 3 \text{ and } q \equiv 7 \pmod 8 \text{ or} \\ & m = 1 \text{ and } q \equiv 1, 5, 7 \pmod 8 \text{ or} \\ & m = 3 \text{ and } q \equiv 3 \pmod 8, \\ \{\pm 1, \pm 2, \pm p, \pm 2p\} & \text{for } m \geqslant 2,\ m \neq 4 \text{ and } q \equiv 1 \pmod 8 \text{ or} \\ & m = 1 \text{ and } q \equiv 3 \pmod 8 \text{ or} \\ & m = 3 \text{ and } q \equiv 5 \pmod 8 \text{ or} \\ & \text{odd } m \geqslant 5 \text{ and } q \equiv 3, 5 \pmod 8. \end{cases} \qquad \square$$

2.2. Generalizations

Let $q - 2^m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ with primes $q, p_1, \ldots, p_n$. Let $E'_{q,m}$: $y^2 = x^3 + 2(2^m - p_1^{\alpha_1} \cdots p_n^{\alpha_n})x^2 + q^2 x$, and let $\phi : E_{q,m} \to E'_{q,m}$ be the two-isogeny defined by $\phi((x, y)) := (y^2/x^2, -y(2^m p_1^{\alpha_1} \cdots p_n^{\alpha_n} + x^2)/x^2)$; let $\hat{\phi}$ denote the dual isogeny. In this section we study the Selmer groups $S^{(\phi)}(E_{q,m}/\mathbb{Q})$ and $S^{(\hat{\phi})}(E'_{q,m}/\mathbb{Q})$. In this case we take $S = \{\infty, 2, q, p_1, \ldots, p_n\}$, $C_d(q, m)$: $dy^2 = d^2 - 2d(q - 2^{m+1})x^2 + q^2 x^4$, and $C'_d(q, m)$: $dy^2 = d^2 + 4d(q - 2^{m+1})x^2 - 2^{m+4}(q - 2^m)x^4$, with $d \in \mathbb{Q}(S, 2) = \langle -1, 2, q, p_1, \ldots, p_n \rangle$.

Proposition 2. *Assume $q = 2^m + p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, with even m and primes $q, p_1, \ldots, p_n$ satisfying $p_i \equiv 1 \pmod 8$ $(i = 1, \ldots, k,\ k \leqslant n)$ and $(\frac{p_i}{p_j}) = 1$ for $i, j = 1, \ldots, k$ $(i \neq j)$. Then*

$$S^{(\phi)}(E_{q,m}/\mathbb{Q}) = \langle q \rangle \quad \text{and} \quad \langle p_1, \ldots, p_k \rangle \subset S^{(\hat{\phi})}\big(E'_{q,m}/\mathbb{Q}\big).$$

Proof. Of course, $(0, 1) \in C_1(q, m)(\mathbb{Q})$ and $(1, 2^{(m+2)/2}) \in C_q(q, m)(\mathbb{Q})$. On the other hand, $C_d(q, m)(\mathbb{R}) = \emptyset$ for $d < 0$, and $C_d(q, m)(\mathbb{Q}_2) = \emptyset$ for even d (take the valuation v_2 of both sides). Similarly $C_{r p_{i_0}}(q, m)(\mathbb{Q}_{p_{i_0}}) = \emptyset$ for $r \in \langle p_1, \ldots, p_{i_0 - 1}, p_{i_0 + 1}, \ldots, p_n, q \rangle$. Hence $S^{(\phi)}(E_{q,m}/\mathbb{Q}) = \langle q \rangle$.

Now fix any p_{i_0}, $1 \leqslant i_0 \leqslant k$. Of course $C'_{p_{i_0}}(q, m)(\mathbb{R}) \neq \emptyset$. By Hensel's Lemma we have $C'_{p_{i_0}}(q, m)(\mathbb{Z}_l) \neq \emptyset$, $l \in \{2, q, p_1, \ldots, p_{i_0 - 1}, p_{i_0 + 1}, \ldots, p_k\}$ (take $x = 0$ and use the assumptions). Lemma 14 in [11] implies $C'_{p_{i_0}}(q, m)(\mathbb{Q}_{p_j}) \neq \emptyset$ for $j = k + 1, \ldots, n$. It remains to prove $C'_{p_{i_0}}(q, m)(\mathbb{Q}_{p_{i_0}}) \neq \emptyset$. If $\alpha_{p_{i_0}} = 1$, then we can apply Lemma 14 in [11]. If $\alpha_{p_{i_0}} \geqslant 2$, then we use Hensel's Lemma. We omit the details. $\square$

2.3. Prime quadratic twists

For any prime r not dividing $2pq$ consider the corresponding quadratic twist $E^{(r)}_{q,p,m}$: $y^2 = x^3 + (p - 2^m)rx^2 - 2^m pr^2x$. Similarly let $E^{(r)'}_{q,p,m}$: $y^2 = x^3 - 2(p - 2^m)rx^2 + (p + 2^m)^2r^2x$, and let $\phi : E^{(r)}_{q,p,m} \to E^{(r)'}_{q,p,m}$ be the two-isogeny defined by

$$\phi((x, y)) = \left(y^2/x^2, -y\left(2^m pr^2 + x^2\right)/x^2\right);$$

let $\hat{\phi}$ denote the dual isogeny. In this section we compute, under suitable assumptions, the corresponding Selmer groups $S^{(\phi)}(E^{(r)}_{q,p,m}/\mathbb{Q})$ and $S^{(\hat{\phi})}(E^{(r)'}_{q,p,m}/\mathbb{Q})$.

Proposition 3. *Fix odd primes p, q satisfying $q - 2^m = p$. Assume $q \not\equiv 1 \pmod 8$ or $q \equiv 1 \pmod 8$ and $m \in \{1, 2, 3\}$. Then we have $S^{(\phi)}(E^{(r)}_{q,p,m}/\mathbb{Q}) \simeq (0)$ and $S^{(\hat{\phi})}(E^{(r)'}_{q,p,m}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ for a positive proportion of primes r.*

Proof. It is enough to check, that $S^{(\phi)}(E^{(r)}_{q,p,m}/\mathbb{Q}) \simeq (0)$ and $S^{(\hat{\phi})}(E^{(r)'}_{q,p,m}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ in the following cases:

$$\text{(i)}\quad q \equiv 1 \pmod 8 \quad \text{and} \quad \begin{cases} m = 1, & r \equiv 5 \pmod 8, \quad \left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = -1, \\ m = 2, 3, & r \equiv 7 \pmod 8, \quad \left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = -1, \end{cases}$$

$$\text{(ii)}\quad q \equiv 3 \pmod 8 \quad \text{and} \quad \begin{cases} m = 1, 2, & r \equiv 5 \pmod 8, \quad \left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = -1, \\ m \geqslant 3 \quad \text{odd}, & r \equiv 7 \pmod 8, \quad \left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = -1, \\ m \geqslant 4 \quad \text{even}, & r \equiv 7 \pmod 8, \quad \left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = 1, \end{cases}$$

$$\text{(iii)}\quad q \equiv 5 \pmod 8 \quad \text{and} \quad \begin{cases} m = 1, 2, 3, & r \equiv 7 \pmod 8, \quad \left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = -1, \\ m \geqslant 4 \quad \text{even}, & r \equiv 3 \pmod 8, \quad \left(\frac{r}{q}\right) = -\left(\frac{p}{r}\right) = 1, \\ m \geqslant 5 \quad \text{odd}, & r \equiv 3 \pmod 8, \quad -\left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = 1, \end{cases}$$

$$\text{(iv)}\quad q \equiv 7 \pmod 8 \quad \text{and} \quad \begin{cases} m = 1, 2, & r \equiv 7 \pmod 8, \quad \left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = -1, \\ m \geqslant 3, & r \equiv 3 \pmod 8, \quad \left(\frac{r}{q}\right) = \left(\frac{p}{r}\right) = 1. \end{cases}$$

Let us summarize the calculations in case (i): $S^{(\hat{\phi})}(E^{(r)'}_{q,p,m}/\mathbb{Q}) = \{1, -2p, 2r, -pr\}$ for $m = 1, 3$, and $S^{(\hat{\phi})}(E^{(r)'}_{q,p,2}/\mathbb{Q}) = \{1, -p, r, -pr\}$ for $m = 2$. On the other hand, $S^{(\phi)}(E^{(r)}_{q,p,m}/\mathbb{Q}) = \{1\}$. Cases (ii)–(iv) are proven by similar arguments. We omit the details. □

Proposition 4. *Fix odd primes p, q satisfying $q - 2^m = p$. Then we have $S^{(\phi)}(E^{(r)}_{q,p,m}/\mathbb{Q}) \simeq (0)$ and $S^{(\hat{\phi})}(E^{(r)'}_{q,p,m}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^3$ for a positive proportion of primes r.*

Proof. The proof follows the same line as the previous one. We omit the details. □

3. Calculation of the root number

It is plain to see that $\Delta(E_{q,p,m}) = 2^{2m+4}p^2q^2$. In particular, $y^2 = x(x - 2^m)(x + p)$ is a global minimal Weierstrass model for $E_{q,p,m}$ for $m \leqslant 3$. In this case the reduction of $E_{q,p,m}$ is additive at 2, multiplicative at p and q, and good at other primes. More precisely, we have the following result.

Lemma 1.

(i) *The reduction at p is split multiplicative iff $p \equiv 1, 3 \pmod 8$ for $m = 1, 3$, or $p \equiv 1, 5 \pmod 8$ for $m = 2$.*
(ii) *The reduction at q is split multiplicative iff $q \equiv 1, 7 \pmod 8$ for $m = 1, 3$, or q any odd prime for $m = 2$.*

Proof. Easy calculations. □

Proposition 5. *We have*

$$\epsilon(E_{q,p,1}) = \begin{cases} 1 & \text{if } p \equiv 3, 5 \pmod 8, \\ -1 & \text{if } p \equiv 1, 7 \pmod 8, \end{cases}$$

$$\epsilon(E_{q,p,2}) = \begin{cases} 1 & \text{if } p \equiv 3, 5, 7 \pmod 8, \\ -1 & \text{if } p \equiv 1 \pmod 8, \end{cases}$$

$$\epsilon(E_{q,p,3}) = \begin{cases} 1 & \text{if } p \equiv 1, 3, 7 \pmod 8, \\ -1 & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Proof. Let $\epsilon_l(E_{q,p,m})$ denote the local root number at l. Lemma 1 combined with Proposition 3(iii) in [14] implies

$$\epsilon_p(E_{q,p,1})\epsilon_q(E_{q,p,1}) = -1$$

and

$$\epsilon_p(E_{q,p,m})\epsilon_q(E_{q,p,m}) = \begin{cases} -1 & \text{if } p \equiv 3 \pmod 4, \\ 1 & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

for $m = 2, 3$. On the other hand, we have (use [5])

$$\epsilon_2(E_{q,p,1}) = \begin{cases} 1 & \text{if } p \equiv 3, 5 \pmod 8, \\ -1 & \text{if } p \equiv 1, 7 \pmod 8, \end{cases}$$

$$\epsilon_2(E_{q,p,2}) = \begin{cases} 1 & \text{if } p \equiv 1, 3, 7 \pmod 8, \\ -1 & \text{if } p \equiv 5 \pmod 8, \end{cases}$$

$$\epsilon_2(E_{q,p,3}) = \begin{cases} 1 & \text{if } p \equiv 3, 5, 7 \pmod 8, \\ -1 & \text{if } p \equiv 1 \pmod 8. \end{cases}$$

The assertion now follows. □

Now let us consider the case $m \geqslant 4$. Then $y^2 = x^3 + (p - 2^m)x^2 - 2^m x$ (respectively $y^2 + xy = x^3 + \frac{p-2^m-1}{4}x^2 - 2^{m-4}px$) is a global minimal Weierstrass model for $E_{q,p,m}$ if $p \equiv 3 \pmod 4$ (respectively if $p \equiv 1 \pmod 4$). In this case the reduction of $E_{q,p,m}$ is multiplicative at p and q, additive at 2 if $p \equiv 3 \pmod 4$, multiplicative at 2 if $p \equiv 1 \pmod 4$ and $m \geqslant 5$, and good at other primes.

Lemma 2.

(i) *Assume $m = 4$. The reduction at q is split multiplicative and the reduction at p is split multiplicative iff $p \equiv 1 \pmod 4$.*
(ii) *Assume $m \geqslant 5$. Then*
  (a) *the reduction at 2 is split multiplicative iff $p \equiv 1 \pmod 8$;*
  (b) *the reduction at p is split multiplicative iff $p \equiv 1, 3 \pmod 8$, m odd or $p \equiv 1, 5 \pmod 8$, m even;*
  (c) *the reduction at q is split multiplicative iff $q \equiv 1, 7 \pmod 8$, m odd or q any odd prime and m even.*

Proof. Easy calculations. □

Proposition 6.

(i) *We have $\epsilon(E_{q,p,4}) = -1$.*
(ii) *Assume $m \geqslant 5$. Then*

$$\epsilon(E_{q,p,m}) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5, 7 \pmod 8. \end{cases}$$

Proof. If $p \equiv 1 \pmod 4$ ($m \geqslant 4$), then we can apply [12, Proposition 2.2] (the case of semistable reduction). If $p \equiv 3 \pmod 4$, then $\epsilon_2(E_{q,p,m}) = -1$ (use [5]) and $\epsilon_p(E_{q,p,m})\epsilon_q(E_{q,p,m}) = -1$ (use Lemma 2 and [14, Proposition 3]). The assertion now follows. □

4. Proofs of the main results

In the proofs of Theorems 1 and 2, and part (iii) of Corollary 2, we shall use the following Weil–Châtelet groups: $WC(E_{q,p,m}/\mathbb{Q}) = E'_{q,p,m}(\mathbb{Q})/\phi(E_{q,p,m}(\mathbb{Q}))$ and $WC(E'_{q,p,m}/\mathbb{Q}) = E_{q,p,m}(\mathbb{Q})/\hat{\phi}(E'_{q,p,m}(\mathbb{Q}))$. They are easily interpreted as the subgroups of the Selmer groups, consisting of homogeneous spaces with rational point (see [16, Section X]). Using the following exact sequences [16, Theorem 4.2, p. 298]

$$0 \to WC(E_{q,p,m}/\mathbb{Q}) \to S^{(\phi)}(E_{q,p,m}/\mathbb{Q}) \to Ш(E_{q,p,m}/\mathbb{Q})[\phi] \to 0,$$

$$0 \to WC\big(E'_{q,p,m}/\mathbb{Q}\big) \to S^{(\hat{\phi})}\big(E'_{q,p,m}/\mathbb{Q}\big) \to Ш\big(E'_{q,p,m}/\mathbb{Q}\big)[\hat{\phi}] \to 0,$$

and [16, Remark 4.7, pp. 300–301]

$$0 \to \frac{E'(\mathbb{Q})[\hat{\phi}]}{\phi(E(\mathbb{Q})[2])} \to WC(E'/\mathbb{Q}) \to \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to WC(E/\mathbb{Q}) \to 0,$$

we obtain the fundamental formula (compare [16, p. 314])

$$r_{q,p,m} = \dim_2 S^{(\phi)}(E_{q,p,m}/\mathbb{Q}) + \dim_2 S^{(\hat{\phi})}\big(E'_{q,p,m}/\mathbb{Q}\big) - \dim_2 Ш(E_{q,p,m}/\mathbb{Q})[\phi] - \dim_2 Ш\big(E'_{q,p,m}/\mathbb{Q}\big)[\hat{\phi}] - 2,$$

where $\dim_2$ denotes $\dim_{\mathbb{F}_2}$.

Proof of Theorem 1. Assume m is even. Then $WC(E_{q,p,m}/\mathbb{Q}) = \{1, q\}$. Hence, using Proposition 1 and the following exact sequences

$$0 \to WC(E_{q,p,m}/\mathbb{Q}) \to S^{(\phi)}(E_{q,p,m}/\mathbb{Q}) \to Ш(E_{q,p,m}/\mathbb{Q})[\phi] \to 0,$$
$$0 \to Ш\big(E'_{q,p,m}/\mathbb{Q}\big)[\hat{\phi}] \to Ш\big(E'_{q,p,m}/\mathbb{Q}\big)[2] \to Ш(E_{q,p,m}/\mathbb{Q})[\phi]$$

we obtain $Ш(E_{q,p,m}/\mathbb{Q})[\phi] = (0)$ and $Ш(E'_{q,p,m}/\mathbb{Q})[2] = Ш(E'_{q,p,m}/\mathbb{Q})[\hat{\phi}]$.

Now assume m is odd and $q \equiv 3, 5 \pmod 8$. Then $Ш(E_{q,p,m}/\mathbb{Q})[\phi] = (0)$ and $Ш(E'_{q,p,m}/\mathbb{Q})[2] = Ш(E'_{q,p,m}/\mathbb{Q})[\hat{\phi}]$.

If $m = 1$, then we have $WC(E'_{q,p,1}/\mathbb{Q}) = S^{(\hat{\phi})}(E'_{q,p,1}/\mathbb{Q})$ for $p \equiv 7 \pmod 8$, hence $Ш(E_{q,p,1}/\mathbb{Q})[\phi] = Ш(E_{q,p,1}/\mathbb{Q})[2]$ in this case. The case $q \equiv 7 \pmod 8$ follows immediately from Proposition 1.

Assume $m \geqslant 5$, and $q \equiv 7 \pmod 8$. Then it is plain that $-p, 2 \in WC(E'_{q,p,m}/\mathbb{Q})$. Consequently $Ш(E'_{q,p,m}/\mathbb{Q})[\hat{\phi}] = (0)$, and $Ш(E_{q,p,m}/\mathbb{Q})[\phi] = Ш(E_{q,p,m}/\mathbb{Q})[2]$. □

Proofs of corollaries. Corollary 1 is an immediate consequence of Theorem 1. Corollary 2(i), (ii), (iv)–(vi) follows from Theorem 1 combining with Propositions 5 and 6. For the proof of part (iii) let us look at C'_{-2}: $2^5 px^4 + 4(p-4)z^2x^2 - (2z^4 + y^2) = 0$. Taking into account Viete's formulas we see that $-2 \in WC(E'_{q,p,2}/\mathbb{Q})$ implies $2^5 p(x_1^2 x_2^2) = -(2z^4 + y^2)$ with $x_1 \in \mathbb{Z} \setminus \{0\}$. Reducing modulo p, we obtain $2z^4 + y^2 \equiv 0 \pmod p$. In particular, $p \equiv 1, 7 \pmod 8$, a contradiction. Similarly, we obtain $2 \notin WC(E'_{q,p,2}/\mathbb{Q})$. Hence $WC(E'_{q,p,2}/\mathbb{Q}) \subset \langle p, -p\rangle$ and the assertion follows from Proposition 5. □

Proof of Theorem 2. Using (the proof of) Proposition 2, we have $WC(E_{q,m}/\mathbb{Q}) = S^{(\phi)}(E_{q,m}/\mathbb{Q}) = \langle q\rangle$, hence $Ш(E_{q,m}/\mathbb{Q})[\phi] = (0)$. Consequently, $Ш(E'_{q,m}/\mathbb{Q})[\hat{\phi}] = Ш(E'_{q,m}/\mathbb{Q})[2]$, and

$$r_{q,m} + \dim_2 Ш\big(E'_{q,m}/\mathbb{Q}\big)[2] = \dim_2 S^{(\hat{\phi})}\big(E'_{q,m}/\mathbb{Q}\big) - 1 \geqslant k - 1. \qquad \square$$

Proof of Theorem 3. Part (i) for $q \equiv 3, 5, 7 \pmod 8$ or $q \equiv 1 \pmod 8$ and $m = 1, 2, 3$ follows immediately from Proposition 3 combining with Dirichlet theorem on primes in arithmetic progressions. Part (ii) is an immediate consequence of Proposition 4 combining with Dirichlet theorem on primes in arithmetic progressions and the parity conjecture. □

Proof of Theorem 4. (i) Use Proposition 3. (ii) Use Proposition 4. (iii) Combine our assumptions with Propositions 3 and 4. □

5. Towards the construction of a set of generators

In this section we describe the method to search for points of infinite order for a (sub)class of elliptic curves considered in this paper. First, let us recall the following conjecture due to Schinzel and Sierpiński [15].

Conjecture. *Let $f_i(x) \in \mathbb{Z}[x]$ $(i = 1, \ldots, s)$ be irreducible and with positive leading coefficients. Assume that there exists no integer $n > 1$ dividing the product $f_1(k) \cdots f_s(k)$ for all integers k. Then there exist infinitely many positive integers l such that $f_1(l), \ldots, f_s(l)$ are prime numbers.*

Let us consider the equation $x^2 - 2^m x - a^2 = 0$ (m and a fixed positive integers). It has integer solutions iff the corresponding discriminant is a square of an integer: it means that the equation $2^{2m-2} + a^2 = b^2$ has to be soluble in integers a, b. It turns out that the pair $(2^{m-k-2}(2^{2k} - 1), 2^{m-k-2}(2^{2k} + 1))$ are integer solutions to the last equation, where k is an integer satisfying $1 \leqslant k \leqslant m - 2$. Consequently, we obtain two solutions to the original equation:

$$x_1 = -2^{m-k-2}\left(2^k - 1\right)^2, \qquad x_2 = 2^{m-k-2}\left(2^k + 1\right)^2.$$

Consider the following families of pairs of quadratic polynomials corresponding to the roots x_1 and x_2:

$$\begin{aligned} f^{(1)}_{m,k}(y) &= y^2 + 2^{m-k-2}\left(2^k - 1\right)^2, \qquad g^{(1)}_{m,k}(y) = y^2 + 2^{m-k-2}\left(2^k + 1\right)^2, \\ f^{(2)}_{m,k}(y) &= y^2 - 2^{m-k-2}\left(2^k + 1\right)^2, \qquad g^{(2)}_{m,k}(y) = y^2 - 2^{m-k-2}\left(2^k - 1\right)^2. \end{aligned}$$

Note that $f^{(1)}_{m,k}(y)$, $g^{(1)}_{m,k}(y)$ are irreducible, and $f^{(2)}_{m,k}(y)$, $g^{(2)}_{m,k}(y)$ are irreducible when $m + k$ is odd. Of course, $f^{(1)}_{m,k}(y)g^{(1)}_{m,k}(y)$ is always divisible by 3 when $m + k$ is odd. Let us check that (for fixed m and k, $m + k$ even) there exists no integer $n > 1$ dividing the product $f^{(1)}_{m,k}(l)g^{(1)}_{m,k}(l)$ for every integer l. If $p \mid f^{(1)}_{m,k}(l)g^{(1)}_{m,k}(l)$ for a prime p and every integer l, then, in particular, $p \mid 2^{2(m-k-2)}(2^{2k} - 1)^2$ (take $l = 0$). But $2 \mid f^{(1)}_{m,k}(0)g^{(1)}_{m,k}(0)$ implies $2 \nmid f^{(1)}_{m,k}(1)g^{(1)}_{m,k}(1)$, and $p \mid 2^{2k} - 1$ implies $p \nmid f^{(1)}_{m,k}(2^{\frac{m-k}{2}})g^{(1)}_{m,k}(2^{\frac{m-k}{2}})$, a contradiction.

The conjecture implies that there exist infinitely many pairs of primes $(p, p + 2^m) = (y^2 + 2^{m-k-2}(2^k - 1)^2, y^2 + 2^{m-k-2}(2^k + 1)^2)$, and consequently, non-torsion rational point on the corresponding elliptic curves $y^2 = x(x - 2^m)(x + p)$.

The same (if $m + k$ is odd) for the second pair of polynomials.

Example. Consider the case $m = 3$. Then $k = 1$, $a = 3$, $b = 5$, and $x_1 = -1$. The pair of polynomials $f^{(1)}_{3,1}(y) = y^2 + 1$, $g^{(1)}_{3,1}(y) = y^2 + 9$ satisfies the assumptions of the conjecture. Therefore we should expect that $(-1, y_{q,p,3}) \in E_{q,p,3}(\mathbb{Q})$ for infinitely many primes p. Here are the initial pairs (p, q): (5, 13), (101, 109), (401, 409), (1601, 1609).

Remarks. (i) The above method sometimes "produces" two independent points. For instance, $(288, 2976), (-144, 5520) \in E_{929,673,8}(\mathbb{Q})$, $(-144, 1618), (648, 2976) \in E_{449,193,8}(\mathbb{Q})$, $(-144, 3120), (648, 15\,624) \in E_{569,313,8}(\mathbb{Q})$.

(ii) The construction described above can be applied to curves $E_{q,m}$. Consider the curve $E_{1721,10}$. The above method "produces" independent points $P_1 = (1152, 16\,512)$, $P_2 = (-576, 10\,560)$, $P_3 = (8712, 793\,848)$: regulator of the subgroup generated by P_1, P_2, P_3 equals 69.37069.

6. Numerical calculations related to the rank

6.1. Empirical distribution of ranks

It is believed that half of all elliptic curves over $\mathbb{Q}$ have rank 0 and half rank 1, with higher ranks occurring in a proportion which is asymptotically zero. Numerical investigations related to the family $x^3 + y^3 = m$ ($m \in \mathbb{N}$, m cubefree) suggest that the expectation may be wrong: here about 23.3% have rank 2 or greater [18]. It turns out that the expectation may also be wrong in the case of our family $E_{q,p,m}$. Here we give some details.

Let $N(x, r)$ denote the number of curves $E_{q,p,m}$ with $q \leqslant x$ and $r_{q,p,m} = r$. Put $n(x, 1) := \frac{N(x,1)}{N(x,+)+N(x,1)}$ and $n(x, +) := \frac{N(x,+)}{N(x,+)+N(x,1)}$, where $N(x, +) := N(x, 0) + N(x, 2)$. Using Corollaries 1 and 2 (hence, assuming the parity conjecture) we obtain Table 1.

Table 1

x	$N(x,+)$	$N(x,1)$	$n(x,+)$	$n(x,1)$
10 000	748	1531	0.328214	0.671786
20 000	1388	2798	0.331581	0.668419
30 000	1974	4043	0.328070	0.671930
40 000	2529	5285	0.323650	0.676350
50 000	3047	6512	0.318757	0.681243
60 000	3607	7668	0.319911	0.680089
70 000	4128	8763	0.320223	0.679777
80 000	4634	9972	0.317267	0.682733
90 000	5160	11 113	0.317090	0.682910
100 000	5699	12 233	0.317812	0.682188
200 000	10 503	23 089	0.312664	0.687336
300 000	15 056	33 519	0.309954	0.690046
400 000	19 545	44 044	0.307364	0.692636

6.2. Numerical generalizations of Theorem 1

For a pair (q, m), where q is an odd prime such that $q - 2^m > 0$, consider an elliptic curve $E_{q,m}$ defined by

$$E_{q,m}\colon\ y^2 = x\big(x - 2^m\big)\big(x + q - 2^m\big).$$

Denote $r_{q,m} = \operatorname{rank} E_{q,m}(\mathbb{Q})$. Here are our numerical observations concerning $r_{q,m}$'s, with $q < 3500$. In our computations we have used Cremona's program MWRANK [3].

(i) $r_{q,m} \leqslant 2$ for $m = 1, 2, 3, 4$.

(ii) Assume $q - 2 = p_1 p_2$ is a product of different primes. If $p_1 \equiv p_2 \equiv 3 \pmod 8$, then $r_{q,1} = 0$ or 2. If $p_1 \equiv p_2 \equiv 5, 7 \pmod 8$, then $r_{q,1} = 0$. We have no example with $p_1 \equiv p_2 \equiv 1 \pmod 8$. If $p_1 \equiv 1 \pmod 8$ and $p_2 \equiv 7 \pmod 8$, then $r_{q,1} = 2$. If $p_1 \equiv 3 \pmod 8$ and $p_2 \equiv 5 \pmod 8$, then $r_{q,1} = 0$. In all the remaining cases we have $r_{q,1} = 1$.

More generally, assume $q-2=p_1\cdots p_k$ is a product of different rational primes. Then

$$r_q \equiv \sum_{i=1}^{k} u(p_i) \pmod 2,$$

where

$$u(p)=\begin{cases} 0 & \text{if } p\equiv 3,5 \pmod 8,\\ 1 & \text{if } p\equiv 1,7 \pmod 8.\end{cases}$$

(iii) Assume $q-2^2=p_1p_2$ is a product of different primes. If $p_1\not\equiv p_2 \pmod 8$, then $r_{q,2}=1$. If $p_1\equiv p_2\equiv 1,3,7 \pmod 8$, then $r_{q,2}=0$. If $p_1\equiv p_2\equiv 5 \pmod 8$, then $r_{q,2}=0$ or 2.

(iv) Assume $q-2^3=p_1p_2$ is a product of different primes. If $p_1\equiv p_2 \pmod 8$, then $r_{q,3}=1$. If $p_1\equiv 3 \pmod 8$ and $p_2\equiv 7 \pmod 8$, then $r_{q,3}=0$. If $p_1\equiv 1 \pmod 8$ and $p_2\equiv 5 \pmod 8$, then $r_{q,3}=2$. In all the remaining four cases we have $r_{q,3}=1$.

(v) Assume $q-2^4=p_1p_2$ is a product of different primes. If $p_1\equiv 1 \pmod 8$ and $p_2\equiv 3 \pmod 8$, then $r_{q,4}=2$. If $p_1\equiv p_2\equiv 5 \pmod 8$ or $p_1\equiv 1 \pmod 8$, $p_2\equiv 5 \pmod 8$, then $r_{q,4}=0$ or 2. In all the remaining cases we have $r_{q,4}=0$.

(vi) Assume $q-2^m=p_1p_2$ is a product of different primes, and $m\geqslant 5$. If $(p_1 \bmod 8,\ p_2 \bmod 8)\in\{(3,5),(3,7),(5,7)\}$, then $r_{q,m}=0$. If $p_1\equiv p_2\equiv 3,5,7 \pmod 8$, then $r_{q,m}=1$. If $p_1\equiv 1 \pmod 8$ and $p_2\equiv 7 \pmod 8$, then $r_{q,m}=2$. If $p_1\equiv 1 \pmod 8$ and $p_2\equiv 3,5 \pmod 8$, then $r_{q,m}=0$ or 2. If $p_1\equiv p_2\equiv 1 \pmod 8$, then $r_{q,m}=1$ or 3. Here are examples of rank 3 elliptic curves: $r_{1777,7}=r_{1721,10}=3$.

7. Lower bounds for the canonical height

Lang [10] has formulated the conjecture which says that the canonical height of a non-torsion point on an elliptic curve E should satisfy $\hat{h}(P)\gg\log|\Delta_E|$. Put $\beta_E:=\frac{\log|\Delta_E|}{\log N_E}$. Hindry and Silverman [7, Theorem 0.3] proved that the canonical height of a non-torsion point on E should satisfy $\hat{h}(P)\geqslant c(\beta_E)\log|\Delta_E|$, where $c(\beta_E):=(20\beta_E)^{-8}\times 10^{-1.1-4\beta_E}$. Hence Lang's conjecture holds true for elliptic curves with universally bounded β_E.

One immediately checks that $\beta_{E_{q,p,m}}<4$, hence $\hat{h}(P)\geqslant 80^{-8}\times 10^{-17.1}\log|\Delta_E|$ for non-torsion points in our family of elliptic curves. Similarly $\beta_{E^{(d)}_{q,p,m}}<7$, hence $\hat{h}(P)\geqslant 140^{-8}\times 10^{-29.1}\log|\Delta_{E^{(d)}}|$ for quadratic twists. Below we prove much sharper inequalities. Similar estimates for the family of congruent number elliptic curves are proved in [1]. We consider global minimal Weierstrass models for $E_{q,p,m}$ as described in Section 3. Let

$$E_0(\mathbb{Q}_r):=\left\{P\in E(\mathbb{Q}_r):\ \tilde{P}\in\tilde{E}(\mathbb{F}_r)_{ns}\right\}$$

be the set (actually, the group) of points of $E(\mathbb{Q}_r)$ with non-singular reduction modulo a prime r. It is well known [17, p. 362] that $E(\mathbb{Q}_r)/E_0(\mathbb{Q}_r)$ is finite; more precisely, it is a cyclic group of order $-v_r(j_E)$ in a case of split multiplicative reduction at r, and has order 1, 2, 3 or 4 otherwise.

Lemma 3. *Let* $P\in E^{(d)}_{q,p,m}(\mathbb{Q})$.

(i) $P\in E^{(d)}_{q,p,m,0}(\mathbb{Q}_r)$ *for* $(r,2pqd)=1$;

(ii) $2P\in E^{(d)}_{q,p,m,0}(\mathbb{Q}_r)$ *for* $r=p,q,p_i$, *where* $p_i\mid d$;

(iii) $2P \in E^{(d)}_{q,p,1,0}(\mathbb{Q}_2)$;

(iv) $2P \in E^{(d)}_{q,p,2,0}(\mathbb{Q}_2)$ *for* $p \not\equiv d \pmod 4$ *or* $p \equiv d \pmod 8$ *and* $4P \in E^{(d)}_{q,p,2,0}(\mathbb{Q}_2)$ *for* $p \equiv d \pmod 4$ *and* $p \not\equiv d \pmod 8$;

(v) $2P \in E^{(d)}_{q,p,3,0}(\mathbb{Q}_2)$;

(vi) $P \in E^{(d)}_{q,p,4,0}(\mathbb{Q}_2)$ *for* $p \equiv d \pmod 4$ *and* $2P \in E^{(d)}_{q,p,4,0}(\mathbb{Q}_2)$ *for* $p \not\equiv d \pmod 4$;

(vii) $2P \in E^{(d)}_{q,p,m,0}(\mathbb{Q}_2)$ *for* $m \geqslant 5$ *and* $p \not\equiv d \pmod 4$;

(viii) $2(m-4)P \in E^{(d)}_{q,p,m,0}(\mathbb{Q}_2)$ *for* $m \geqslant 5$ *and* $p \equiv d \pmod 4$.

Proof. One uses Tate's algorithm (see [17]) and considers possible types of the groups $E(\mathbb{Q}_r)/E_0(\mathbb{Q}_r)$ depending on the Kodaira symbol (compare [17, Table 4.1, p. 365]).

Let us summarize the calculations. First note that $\Delta(E^{(d)}_{q,p,m}) = 2^{2m+4}p^2q^2d^6$. If $(r, 2pqd) = 1$, then the Kodaira symbol is I_0. If $r \in \{p, q\}$, then the Kodaira symbol is I_2. If $r = p_i$ (p_i a prime dividing d), then the Kodaira symbol is $I_0^\star$. The remaining case $r = 2$ splits into several subcases: (a) $m = 1$, then the Kodaira symbol is III, (b) $m = 2$ and $pd \equiv 3 \pmod 4$, then the Kodaira symbol is $I_0^\star$; $m = 2$ and $pd \equiv 1 \pmod 4$, then the Kodaira symbol is $I_1^\star$ (if $pd \equiv 1 \pmod 8$, then the Tamagawa number $c = 2$, otherwise $c = 4$), (c) $m \geqslant 3$ and $pd \equiv 3 \pmod 4$, then the Kodaira symbol is $I^\star_{2(m-2)}$, (d) $m = 3$ and $pd \equiv 1 \pmod 4$, then the Kodaira symbol is $III_1^\star$, (e) $m = 4$ and $pd \equiv 1 \pmod 4$, then the Kodaira symbol is I_0, (f) $m \geqslant 5$ and $pd \equiv 1 \pmod 4$, then the Kodaira symbol is $I_{2(m-4)}$.

Now it is enough to consider possible types of the groups $E(\mathbb{Q}_r)/E_0(\mathbb{Q}_r)$ depending on the Kodaira symbol. We omit the details. □

Proposition 7. *Let* $P \in E^{(d)}_{q,p,m}(\mathbb{Q})$ *be a non-torsion rational point.*

(i) *If* $p \not\equiv d \pmod 4$ *or* $p \equiv d \pmod 4$, $m = 1, 3$ *or* $p \equiv d \pmod 8$, $m = 2$, *then*

$$\hat{h}(P) \geqslant \frac{1}{16}\log\bigl(2^m qd^2\bigr); \tag{7.1}$$

(ii) *If* $p \equiv d \pmod 4$, $p \not\equiv d \pmod 8$, $m = 2$, *then*

$$\hat{h}(P) \geqslant \frac{1}{64}\log\bigl(4qd^2\bigr); \tag{7.2}$$

(iii) *If* $p \equiv d \pmod 4$, $m = 4$, *then*

$$\hat{h}(P) \geqslant \frac{1}{16}\log\bigl(qd^2\bigr); \tag{7.3}$$

(iv) *If* $p \equiv d \pmod 4$, $m \geqslant 5$, *then*

$$\hat{h}(P) \geqslant \frac{1}{16(m-4)^2}\log\bigl(2^{m-4}qd^2\bigr). \tag{7.4}$$

Proof. We will first estimate the archimedean contribution $\hat{h}_\infty$ to the canonical height by using Tate's series. Arguing as in [1, p. 192] we obtain:

(a) if $p \not\equiv d \pmod 4$ or $p \equiv d \pmod 4$, $m \leqslant 3$ then (take $z = (1 + 2^m pd^2t^2)^2$)

$$0 \leqslant \hat{h}_\infty(P) + \frac{1}{12}\log|\Delta_{E^{(d)}}| - \frac{1}{4}\log\bigl(x(P)^2 + 2^m pd^2\bigr); \tag{7.5}$$

(b) if $p \equiv d \pmod 4$, $m \geqslant 4$ then (take $z = (1 + 2^{m-4} pd^2t^2)^2$)

$$0 \leqslant \hat{h}_\infty(P) + \frac{1}{12}\log|\Delta_{E^{(d)}}| - \frac{1}{4}\log\bigl(x(P)^2 + 2^{m-4} pd^2\bigr). \tag{7.6}$$

Let $Q = 2P$. From Lemma 3 it follows that $Q \in E^{(d)}_{q,p,m,0}(\mathbb{Q}_r)$ for any rational prime r in the following cases: $p \not\equiv d \pmod 4$ or $p \equiv d \pmod 4$, $m = 1, 3, 4$ or $p \equiv d \pmod 8$, $m = 2$. In these cases the local height of Q at r is given by the formula [17, Theorem 4.1]

$$\hat{h}_r(Q) = \frac{1}{2}\max\bigl\{0, -v_r\bigl(x(Q)\bigr)\bigr\} + \frac{1}{12}v_r(\Delta), \tag{7.7}$$

where we denote $v_r(x) = \operatorname{ord}_r(x)\log(r)$. Writing $x(Q) = \frac{\alpha}{\delta^2}$, and combining (7.5) (respectively (7.6)) and (7.7) we obtain: in case (a)

$$\hat{h}(Q) \geqslant \frac{1}{4}\log\bigl(\alpha^2 + 2^m p\delta^4\bigr) \geqslant \frac{1}{4}\log\bigl(2^m qd^2\bigr); \tag{7.8}$$

in case (b)

$$\hat{h}(Q) \geqslant \frac{1}{4}\log\bigl(\alpha^2 + 2^{m-4} p\delta^4\bigr) \geqslant \frac{1}{4}\log\bigl(2^{m-4} qd^2\bigr). \tag{7.9}$$

Now $\hat{h}(Q) = 4\hat{h}(P)$, and the assertions (i) and (iii) follow. The remaining cases follow under the same lines. □

We give a direct application of Proposition 7. Put $l_q(P) := \frac{16\hat{h}(P)}{\log(2^m q)}$. Consider $E_{13,5,3}$: Theorem 1 implies $r_{13,5,3} \leqslant 1$; Cremona's program MWRANK [3] actually gives $r_{13,5,3} = 1$. Take $P = (-1, 6) \in E_{13,5,3}(\mathbb{Q})$. Then $l_{13}(P) = 6.55$, and $P \notin 2E_{13,5,3}(\mathbb{Q})$, whence P generates the free part of $E_{13,5,3}(\mathbb{Q})$.

8. The analytic order of Ш

We conclude with examples of rank zero elliptic curves $E_{q,p,m}$ having conjectural values of $|Ш(E_{q,p,m}/\mathbb{Q})|$ equal to m^2, $m = 1, \ldots, 7, 9$. We have computed (using the package COMPUTEL [4]), the following quantity:

$$S_{q,p,m} := \frac{L(E_{q,p,m}, 1)}{\Omega_{E_{q,p,m}}} \times \frac{|E_{q,p,m}(\mathbb{Q})_{\mathrm{tors}}|^2}{c_{E_{q,p,m}}},$$

where $c_{E_{q,p,m}}$ is the Tamagawa number, $E_{q,p,m}(\mathbb{Q})_{\mathrm{tors}}$ denotes the torsion subgroup, and $\Omega_{E_{q,p,m}}$ is the real period. According to the Birch and Swinnerton–Dyer conjecture we should have $S_{q,p,m} = |Ш(E_{q,p,m}/\mathbb{Q})|$.

$$S_{5,3,1} = 1, \qquad S_{73,41,5} = 4, \qquad S_{109,107,1} = 9, \qquad S_{433,401,5} = 16,$$
$$S_{1789,1787,1} = 25, \qquad S_{2113,2081,5} = 36, \qquad S_{2341,2339,1} = 49, \qquad S_{7549,7547,1} = 81.$$

We can confirm that the 2-rank of Ш is 2 for the curves with $S = 4$ (respectively $S = 36$), which is consistent with $|Ш| = 4$ (respectively $|Ш| = 36$) and $Ш \simeq (\mathbb{Z}/2\mathbb{Z})^2$ (respectively $Ш \simeq (\mathbb{Z}/6\mathbb{Z})^2$). The curves with $S = 16$ also have the 2-rank of Ш equal to 2, suggesting that for these curves we have $Ш \simeq (\mathbb{Z}/4\mathbb{Z})^2$ rather than $(\mathbb{Z}/2\mathbb{Z})^4$.

Acknowledgment

We thank an anonymous referee for the constructive criticism and comments which improved the final version.

References

[1] A. Bremner, J.H. Silverman, N. Tzanakis, Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$, J. Number Theory 80 (2000) 187–208.
[2] G. Coogan, J. Jiménez-Urroz, Mordell–Weil ranks of quadratic twists of pairs of elliptic curves, J. Number Theory 96 (2002) 388–399.
[3] J.E. Cremona, http://www.maths.nott.ac.uk/personal/jec/ftp/progs/.
[4] T. Dokchitser, COMPUTEL—Computing special values of L-functions, Number Theory ftp/calculator programs.
[5] E. Halberstadt, Signes locaux des courbes elliptiques en 2 et 3, C. R. Acad. Sci. Paris 326 (1998) 1047–1052.
[6] G.H. Hardy, J.E. Littlewood, Partitio numerorum III: On the expression of a number as a sum of primes, Acta Math. 44 (1923) 1–70.
[7] M. Hindry, J.H. Silverman, The canonical height and integral points on elliptic curves, Invent. Math. 93 (1988) 419–450.
[8] H. Iwaniec, P. Sarnak, The non-vanishing of central values of automorphic L-functions and Landau–Siegel zeros, Israel J. Math. 120 (2000) 155–177.
[9] A.W. Knapp, Elliptic Curves, Math. Notes, vol. 40, Princeton Univ. Press, Princeton, 1992.
[10] S. Lang, Elliptic Curves: Diophantine Analysis, Grundlehren Math. Wiss., vol. 231, Springer, 1978.
[11] J.R. Merriman, S. Siksek, N.P. Smart, Explicit 4-descents on an elliptic curve, Acta Arith. 77 (1996) 385–404.
[12] A. Nitaj, Invariants des courbes de Frey–Hellegouarch et grands groupes de Tate–Shafarevich, Acta Arith. 93 (2000) 303–327.
[13] K. Ono, C. Skinner, Non-vanishing of quadratic twists of modular L-functions, Invent. Math. 34 (1998) 651–660.
[14] D.E. Rohrlich, Variation of the root number in families of elliptic curves, Compos. Math. 87 (1993) 119–151.
[15] A. Schinzel, W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, Acta Arith. 4 (1958) 185–208.
[16] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer, New York, 1985.
[17] J.H. Silverman, Advances Topics in the Arithmetic of Elliptic Curves, Springer, New York, 1994.
[18] D. Zagier, G. Kramarz, Numerical investigations related to the L-series of certain elliptic curves, J. Indian Math. Soc. 52 (1987) 51–69.